IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application. No.	: 10/045,893	Confirmation No.	: 3131
1st Named Inventor	: Adusumilli	Art Unit	: 2134
Filed	: 01/12/2002	Examiner	: Brown, Christopher J.
Docket No.	: 42390.P12318X	Customer No.	: 7590

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF IN RESPONSE TO EXAMINER'S ANSWER
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicants (hereafter "Appellants") hereby submit this Reply Brief in response to the Examiner's Answer mailed in the above-identified case on May 21, 2009. The fees required under §41.20 for filing this Reply Brief are dealt with in the accompanying Transmittal of Appeal Brief. Appellants respectfully request consideration of this Reply Brief by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application.

An oral hearing is not desired.

REMARKS

REJECTION OF CLAIMS 33-36, 38, 40, 42, 43, 45, 48, 50-52, AND 54-59 UNDER 35 U.S.C. § 103(A) AS BEING UNPATENTABLE OVER U.S. PATENT NO. 6,571,221 TO STEWART (HEREINAFTER "STEWART") IN VIEW OF U.S. PUB. NO. 2002/0099957 BY KRAMER (HEREINAFTER "KRAMER") IN VIEW OF U.S. PATENT NO. 7,099,284 TO HALME (HEREINAFTER "HALME") IS BELIEVED TO BE IMPROPER

GROUP I: CLAIMS 33-55, 59, and 60

Appellants respectfully submit that the claims of Group I are allowable over Stewart, Kramer, and Halme.

Claim 33 pertains to:

> "*An apparatus to reside in a data center coupled between a public network and a server of the data center, the apparatus comprising:*
>
> *a first interface to the public network to receive Secure Sockets Layer (SSL) encrypted data from at least one wired client device and to receive Wireless Transport Layer Security (WTLS) encrypted data from at least one wireless client device;*
>
> *client-type determining logic to determine whether a client device requesting a secure connection is a wired client device or a wireless client device;*
>
> *logic to perform a wired authentication to establish the secure connection when it is determined that the requesting client device is the wired client device;*
>
> *logic to perform a wireless authentication to establish the secure connection when it is determined that the requesting client device is the wireless client device;*
>
> ***logic to convert the SSL encrypted data to an unencrypted format and to convert the WTLS encrypted data to an unencrypted format; and***
>
> ***a second interface to provide the data in the unencrypted formats to the server of the data center***".

Stewart, Kramer and Halme do not disclose these limitations or render them obvious.

Stewart pertains to a network communication service with an improved subscriber model using digital certificates. See e.g., the Title. However, Stewart does not disclose or render obvious the claimed apparatus **to reside in a data center coupled between a public network and a server of the data center** that comprises **a first interface to the public network** to receive **SSL** and **WTLS** encrypted data, and that has **logic to convert the SSL and WTLS encrypted data to unencrypted formats**, and that has **a second interface to provide the data in the unencrypted formats to the server of the data center**, in combination with the other claim limitations.

Firstly, as understood by Applicants, Stewart does not disclose logic to convert the SSL and WTLS encrypted data to unencrypted formats. In fact, Stewart does not even appear to mention "WTLS". The Examiner appears to agree, since on page 3 of the present Office Action, the Examiner has stated that "*Stewart does not teach SSL, WTLS or converting encrypted data to an unencrypted format*".

Secondly, in rejecting claim 33, the Examiner has relied upon features of **both the hybrid wired and wireless access point 124 and the service provider 140.** See e.g., page 4 of the present Final Office Action. For example, on page 4 of the present Final Office Action, the Examiner references column 8, lines 47-55 which describes hybrid wired and wireless access point 124, and column 14, lines 29-44 which describes actions by network or service provider 140. However, Applicants respectfully submit that it is inappropriate and the Examiner has not sufficiently articulated why this could or would be appropriate. The hybrid wired and wireless access point 124 and the service provider 140 are different components and are separated by a centralized network 130. Column 8, line 65 indicates that network 130 is preferably the **Internet**. Different components 124, 140 separated by network 130, preferably the Internet, do not meet the limitations of claim 33. Claim 33 recites that the apparatus is to reside in a data center coupled between a public network and a server of the data center and has the claimed first interface to the

public network and the claimed second interface to provide the data in the unencrypted formats to the server of the data center. The hybrid wired and wireless access point 124 does not reside **in a data center coupled between a public network and a server of the data center** and does not have a second interface to provide the data in the **unencrypted** formats to the server of the data center.

Thirdly, Stewart does not disclose or render obvious an apparatus that is to reside in a data center coupled between a public network and a server of the data center and has the claimed first interface to the public network and the claimed second interface to provide the data in the unencrypted formats to the server of the data center. As discussed above, the hybrid wired and wireless access point 124 does not reside **in a data center coupled between a public network and a server of the data center** and does not have a second interface to provide the data in the **unencrypted** formats to the server of the data center. Moreover, Stewart does not disclose that the service provider 140 have a second interface to provide data in the unencrypted formats to a server of a data center.

Kramer does not remedy all of what is missing from Stewart. Kramer discusses establishing a secure connection with a private corporate network over a public network. See e.g., the Title. Kramer discusses in paragraph [0050] "*the external client secures the connection 430*" and that "*The security for the connection may be provided by using Secured Socket Layer (SSL) protocol or Wireless Transport Layer Security (WTLS) security*". However, as understood by Applicants, the SSL and the WTLS are used by the "*external client*" (e.g., **external client 340**). The external client 340 does not reside in a data center coupled between a public network and a server of the data center. Furthermore, Kramer does **not disclose** that the VPN access server 314 has logic to convert the SSL encrypted data to an unencrypted format and to **convert the WTLS** encrypted data to an unencrypted format. Kramer does not even disclose that the VPN access server 314 **receive WTLS** data. It should not be assumed that just because the

external client uses WTLS that the VPN access server 314 would **receive WTLS**. Rather, as understood by Applicants, **conversion from WTLS to another format (e.g., SSL)** would typically be performed before reaching the VPN access server 314 e.g., in a WAP gateway of the like. (For example, a cell phone may use WTLS but a server in communication with the cell phone would typically not receive WTLS but rather SSL or some other wired format after the WTLS data was converted, for example, in a WAP gateway.)

In the response to arguments section at the bottom of page 9 of the Examiner's Answer, the Examiner has asserted that instead, "*A dedicated public line may be used with a wireless client, and the WAP conversion may take place at the entrance to the corporate network, along the lines of the present invention*". See e.g., the last two lines on page 9 and the first two lines on page 10 of the Examiner's Answer.

The Examiner has asserted that such a method is taught by Kramer (see e.g., page 10, line 4 of the Examiner's Answer). Appellants respectfully disagree and submit that Kramer does not teach such a method. Kramer does not even mention a "*WAP conversion*", let alone that "*the WAP conversion may take place at the entrance to the corporate network*". The words "*WAP conversion*" simply are not used in Kramer. Moreover, Kramer does not mention the "*dedicated public line*" referred to by the Examiner. Accordingly, Kramer does not teach what the Examiner has relied upon Kramer as teaching.

Kramer does not teach a conversion prior to the VPN access server, however this is not surprising since Kramer has a very limited discussion of SSL and WTLS. The fact that Kramer does not elaborate on SSL and WTLS, would seem to indicate that Kramer intends the SSL and WTLS to operate **conventionally**. In fact, Kramer discusses in paragraph [0050] that "*Connections may be secured by conventional (emphasis added)*

encryprion/decryption crypts...". As discussed above, the convention approach known to Applicants is to convert the WTLS prior to the VPN access server 314, and the Examiner has not provided evidence of an alternate approach. Moreover, the Examiner has admitted that "*Appellant is correct that a WAP gateway typically (emphasis added) converts a WTLS request ...*". See e.g., the last two lines on page 9 of the Examiner's Answer. Accordingly, as understood by Applicants, it stands to reason that the **conventional** approach employed in Kramer would be to convert WTLS prior to the WTLS reaching VPN access server 314, as is **typically** done.

Accordingly, since Kramer teaches to secure the connections by a "***conventional***" approach, and since the Examiner admits that "***typically***" a WAP gateway converts a WTLS request, Appellants respectfully submit that such a conversion from WTLS to another format prior to the VPN access server 314 is clearly disclosed in Kramer.

In any event, the Examiner has not provided a reference, or sufficient evidence, to support his assertion that (at the time of filing of the present patent application) it was well known that "*A dedicated public line may be used with a wireless client, and the WAP conversion may take place at the entrance to the corporate network, along the lines of the present invention*".

Accordingly, Appellants respectfully maintain their position that the WTLS data discussed in Kramer would be converted away from WTLS prior to reaching the private corporate network 310.

Accordingly, Kramer does not appear to disclose **an apparatus to reside in a data center coupled between a public network and a server of the data center** that includes a first interface to the public network to receive SSL data and to receive **WTLS data**. Additionally, Kramer does not appear to disclose **an apparatus to reside in a data center coupled between a public network and a server of the data center** that

includes logic to convert the SSL encrypted data to an unencrypted format and to convert the WTLS encrypted data to an unencrypted format.

As discussed above, Stewart also does not disclose such an apparatus.

Halme does not remedy all of what is missing from Stewart and Kramer. Halme discusses a data transmission control and performance monitoring method of an IPSEC link in a virtual private network. See e.g., the Title. However, Halme does not disclose or render obvious an apparatus **to reside in a data center coupled between a public network and a server of the data center** that comprises **a first interface to the public network** to receive **SSL** and **WTLS** encrypted data, and that has **logic to convert the SSL and WTLS encrypted data to unencrypted formats**, and that has **a second interface to provide the data in the unencrypted formats to the server of the data center**, in combination with the other claim limitations.

Accordingly, Stewart, Kramer and Halme do not disclose or render obvious the claimed apparatus **to reside in a data center coupled between a public network and a server of the data center** that comprises **a first interface to the public network** to receive **SSL** and **WTLS** encrypted data, and that has **logic to convert the SSL and WTLS encrypted data to unencrypted formats**, and that has **a second interface to provide the data in the unencrypted formats to the server of the data center**, in combination with the other claim limitations.

Accordingly, even if combined, the references do not disclose all limitations.

Moreover, there is no suggestion or motivation to make the Examiner's proposed combination. Furthermore, the Examiner has not articulated with enough detail what the exact combination would be, or why it would be obvious to make this particular combination. It would seem that modifications to the references not taught in the art

would likely be necessary in order to modify the references in the manner proposed by the Examiner.

Appellants respectfully submit that it is inappropriate to use the claim as an instruction manual or template to piece together the teachings of the prior art so that the claim is rejected as being. Appellants respectfully submit that it is inappropriate to use hindsight reconstruction to pick and choose among seemingly isolated disclosures in the prior art to deprecate the claim.

For at least one or more of these reasons, claim 33, and its dependent claims, are believed to be allowable over Stewart, Kramer and Halme.

Independent claims 42 and 50, and their respective dependent claims, are believed to be allowable for one or more similar reasons.

GROUP II: CLAIMS 56-58

Appellants respectfully submit that the claims of Group II are allowable over Stewart, Kramer, and Halme.

Claim 56 pertains to:

> *"An apparatus comprising:*
>
> ***a network interface** to receive **Secure Sockets Layer (SSL) data** from a wired device through a public network and **Wireless Transport Layer Security (WTLS) data** from a wireless device **through a public network;***
>
> ***Public Key Infrastructure (PKI) logic** to establish a secure connection with the wired device;*
>
> ***Wireless Public Key Infrastructure (WPKI) logic** to establish a secure connection with the wireless device;*
>
> ***SSL logic** to convert the SSL data to another format;*
>
> ***WTLS logic** to convert the WTLS data to another format; and*

a second interface to provide the data converted from the SSL and WTLS formats to a server over a private network".

Stewart, Kramer and Halme do not disclose these limitations or render them obvious. In particular, Stewart, Kramer and Halme do not disclose or render obvious an apparatus that has **a network interface to receive SSL data and WTLS data through a public network, and that has a second interface to provide data converted from the SSL and WTLS formats to a server over a private network.** The discussion above is pertinent to this point, and for brevity will not be repeated.

In addition, Stewart, Kramer and Halme do not disclose or render obvious an apparatus that has a network interface to receive SSL data and WTLS data through a public network, and that has a second interface to provide data converted from the SSL and WTLS formats to a server over a private network, and that also has **Public Key Infrastructure (PKI) logic and Wireless Public Key Infrastructure (WPKI) logic. In particular, neither Stewart, Kramer, or Halme, appear to even mention a Wireless Public Key Infrastructure (WPKI) logic, let alone the particular claimed WPKI logic in the particular claimed apparatus.**

Accordingly, even if combined, the references do not disclose all limitations.

Moreover, there is no suggestion or motivation to make the Examiner's proposed combination. Furthermore, the Examiner has not articulated with enough detail what the exact combination would be, or why it would be obvious to make this particular combination. It would seem that modifications to the references not taught in the art would likely be necessary in order to modify the references in the manner proposed by the Examiner.

Appellants respectfully submit that it is inappropriate to use the claim as an instruction manual or template to piece together the teachings of the prior art so that the

claim is rejected as being. Appellants respectfully submit that it is inappropriate to use hindsight reconstruction to pick and choose among seemingly isolated disclosures in the prior art to deprecate the claim.

For at least one or more of these reasons, claim 56 and its dependent claims are believed to be allowable over Stewart, Kramer and Halme.

CONCLUSION

Based on the foregoing, Appellants request that the Board overturn the rejection of all pending claims and hold that all of the claims of the present application are allowable.

Appellants respectfully petition for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17 for such an extension.

Please charge any shortages and credit any overpayment to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: July 21, 2009

By Brent E. Vecchia

Brent E. Vecchia, Reg. No. 48,011
Tel.: (303) 740-1980 (Mountain Time)

1279 Oakmead Parkway
Sunnyvale, California 94085-4040